ASSESSMENT

Application Security Assessment

Be Confident That Your Applications Are Protected

The continuous change in business goals and technology needs can leave a company unsure of their security posture. Many companies focus their security resources on networks and servers as the first layer into a company's biggest assets. But what happens if that layer of security is breached or if bad actors already exist inside your network or server?

That is where Catapult's Application Security Assessment comes in.

Security experts provide you with an analysis of your source code and environment. We help you understand the security landscape of your custom or legacy applications and identify the risk you may have if a hacker were to gain access to your network.

During the Application Security Assessment, Catapult security experts review your current application architecture and the posture of your network. They also look for application hosting vulnerabilities and investigate your authentication and authorization methodology. Furthermore, they analyze your static code for issues ranging from information leakage to injection vulnerabilities.

WHY YOU SHOULD GET IT

Custom applications automate and incorporate critical business processes and work with confidential information that must be protected. When security mechanisms are missing, implemented incorrectly, or contain special backdoors left open by developers, your business can be exploited. The risk can be enormous if bad actors gain unauthorized access to your custom applications.

WHAT YOU GET

The Application Security Assessment provides you with guidance to ensure your application code minimizes vulnerabilities and protects your sensitive data. We review your network and create a recommendation roadmap to improve your application security posture. The assessment of a single application takes 1-2 weeks to complete. An assessment of a set of applications takes between 4 -8 weeks.

IN-PERSON SECURITY FINDINGS BRIEFING

APPLICATION SECURITY ASSESSMENT FINDINGS DOCUMENT

A comprehensive review of your current application status, including any risky activities or vulnerabilities detected.

RECOMMENDED APPLICATION SECURITY REMEDIATION ROADMAP

A full report that outlines the findings and the recommendations on remediation and implementation of specific protection

TYPICAL FINDINGS

- SQL injection
- Error handling vulnerabilities
- Information Leakage
- URLs exposing sensitive information
- Stored data protection issues
- Password vulnerabilities
- Insecure user identity management

Catapult

How can we help you?
www.catapultsystems.com
1-800-528-6248 info@CatapultSystems.com